IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, April 2024

Anomaly Detection System

Prof. K. G. Jagtap[1], Shreeram Shinde[2], Akshay Adhav[3], Sahil Kadambande[4]

Professor, Department of AI & ML [1]

Student, Department of AI & ML[2,3,4]

AISSMS Polytechnic, Pune, India

Abstract: *An "Anomaly Detection System" is an software/hardware application that monitors the activity of an network and alerts the user, of any activity that seems to be malicious or strange. The classification between an malicious traffic and normal traffic is done based on the set of rules that are pre-defined. An Anomaly Detection often referred to an IDS reduces the work performed by analyst to monitor network and automates the process of monitoring network traffic to detect anomaly in network traffic data. The implemented Anomaly Detection System takes into consideration various machine learning algorithms and detects abnormal traffic which can also be called as anomaly.*

Keywords: Anomaly, Anomaly Detection System, Denial Of Service, Random Forest, KNN Algorithm, Support Vector Machine.

REFERENCES

[1] Hurley, T.; Perdomo, J.E.; Perez-Pons, "A. HMM-Based Intrusion Detection System for Software Defined Networking. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 617–621.

[2] Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, "Q. A Deep Learning Approach to Network Intrusion Detection", IEEE Trans. Emerg. Top. Comput. Intell. 2018, 2, 41– 50.

[3] Gomez, J.; Gil, C.; Banos, R.; Marquez, A.L.; Montoya, F.G.; Montoya, M.G. A,"Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network Intrusion detection systems", Soft Comput. 2013, 17, 255–263.

[4] Sangeetha, S.; Gayathri devi, B.; Ramya, R.; Dharani, M.K.; Sathya, P. Signature Based Semantic Intrusion Detection System on Cloud. In Information Systems Design and Intelligent Applications; Mandal, J.K., Satapathy, S.C., Kumar Sanyal, M., Sarkar, P.P., Mukhopadhyay, A., Eds.; Springer: New Delhi, India, 2015; pp. 657–666.

[5] Dey, S.K.; Rahman, M.M. , "Effects of Machine Learning Approach in Flow-Based Intrusion Detection on Software-Defined Networking", IEEE 2020

[6] Vipin, Das & Vijaya, Pathak & Sattvik, Sharma &Sreevathsan& MVVNS. Srikanth & Kumar T, Gireesh, "Network Anomaly Detection System Based On Machine Learning Algorithms , International Journal of Computer Science & Information Technology, 2010

[7] Choi, J & Choi, Chang & Ko, Byeongkyu& Choi, D & Kim, "Detecting web based Ddos attack using mapreduce operations in cloud computing environment " Journal of Internet Services and Information Security, 2013

[8] Baig, Zubair & Baqer, M & Khan, Asad, "A Pattern Recognition Scheme for Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks", 2006

[9] Analyzing Log Files for Post-mortem Intrusion Detection Gamboa, Karen & Monroy, Raúl & Trejo, Luis & Aguirre Bermúdez, Eduardo & Mex-Perera, Carlos. (2012), IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)

[10] Network Traffic Analysis and Intrusion Detection Using Packet Sniffer Qadeer, Mohammed & Iqbal, Arshad & Zahid, Mohammad & Siddiqui, Misbahur, Communication Software and Networks

DOI: 10.48175/568